Годишник на секция "Информатика"
Съюз на учените в България
Том 7, 2014, 41–50

Annual of "Informatics" Section
Union of Scientists in Bulgaria
Volume 7, 2014, 41–50

ОБОБЩЕНОМРЕЖОВ МОДЕЛ НА АВТОРИЗАЦИЯ В КОРПОРАТИВЕН СЪРВЪР И МРЕЖА С ПОМОЩТА НА МОБИЛНИ УСТРОЙСТВА

Христо Панайотов

Университет „Проф. д-р Асен Златаров, Бургас
e-mail: itko@btu.bg

Резюме: В статията е представен обобщеномрежови модел на автентификация в корпоративен сървър и мрежа с помощта на мобилни устройства. Той може да се използва за анализ и оптимизира на комуникацията.
Ключови думи: Обобщена мрежа, корпоративен сървър, мобилни устройства.

1 Въведение

Защитата на данните в компютърните мрежи става един от най-важните и дискутирани проблеми в съвременните информационно-изчислителни системи. В няколко статии авторът разглежда използването на мобилните комуникации за повишаване на сигурността при предаването на конфиденциални данни [3, 4, 9]. В [8] е представен обобщеномрежови модел (ОМ, [1, 2]) на процеса на електронно разплащане през интернет. В [6] са моделирани криптиращи протоколи за електронни разплащания. В [4] е разработен обобщеномрежови модел на работата на работна станция в GSM-базирана станция за електронна търговия. В настоящата работа е представен обобщеномрежов модел на на автентификация в корпоративен сървър и мрежа с помощта на мобилни устройства.

На настоящия етап могат да бъдат формулирани три основни задачи, решаването на които би довело до по-висока надежност при функцнирането им.

На първо място – целокупността на данните. Защита от хардуерни и софтуерни инциденти, водещи до загуба на информация или до нейното пълно или частично унищожение. Второ – конфиденциалността на информацията в рамките на конкретната фирма или организация. На трето място – достъпността на информацията съобразно авторизацията на всеки от ползвателите ѝ.

Разглеждайки проблемите, свързани със защитата на данните в мрежови среди, естествено възниква въпросът за класифициране на причините за повредите и несанкционирания достъп, водещи до загубата им или тяхното нежелателно изменение. Това могат да бъдат повреди в оборудването (кабелни мрежи, дискови системи, сървъри, работни станции), загуби на информация вследствие на инициирани компютърни вируси, неправилно съхранение на архивирани данни, нарушение на правата на достъп, както и некоректна работа на ползвателите и обслужващия персонал. Изброените дотук причини за нарушената работа в мрежата водят до необходимостта от създаване на различни по вид и естество средства и методи за защита на информацията. Условно, те биха могли да бъдат систематизирани в три насоки:

1. Средства за физическа защита;
2. Програмни средства (антивирусни програми, системи за разграничаване на пълномощията, софтуер за контрол на достъпа);
3. Административни мерки за защита (достъп до помещения, разработка на стратегии за безопасност на фирмата и т.н.).

Едно от средствата за физическа защита са системите за архивиране и дублиране на информацията. В локалните мрежи с един два сървъра най-често някой от тях играе ролята на архиватор, естествено при наличие на свободен слот от дискова памет или съществуващ специализиран архивиращ хардуер. При големите корпоративни мрежи е необходимо инсталирането на специализиран архивиращ сървър, който автоматично да архивира информацията от дисковите носители на работните сървъри, както и от работни станции, ползващи собствен софтуер и данни. Гореизброените мероприятия би трябвало да се дефинират и организират от системния администратор на мрежата – тяхната периодичност, обхват и отчет на логовете. Доста фирми се насочват към създаването на софтуер за архивиране, като един от най-популярните и ползвани е SAS (Storage Express System) на Intel.

Наскоро друга популярна компания Acronis, крупен производител на програмно осигуряване за архивиране на данни, пусна в продажба нови програмни продукти от семейство Acronis Recovery, предназначени за архивиране и възстановяване на данни от популярни СУБД и Microsoft Exchange. От СУБД се поддържат Oracle и SQL Server. Acronis Recovery се базира на съществуващата архитектура на Acronis True Image, предназначен за създаване на пълни архивни копия на всички данни на сървърите под управление на Windows и Linux. В Acronis твърдят, че новият продукт позволява на ИТ мениджърите и администратори на бази данни бързо да правят архивни копия или да възстановят данни до момента на аварията. Към момента е налична само версия за SQL Server, а други две версии ще се появят в близко време.

Друг важен аспект на сигурността е борбата с компютърните вируси – тема толкова обширна за дискутиране колкото е нейната значимост. Най-често използваните средства за предотвратяване на проникването на вируси естествено са антивирусните програми – непрекъснато разширяващи обсег и претенции за сигурност. Напоследък се

забелязва тенденция към съчетаване на програмните методи с апаратни такива. Това са специални антивирусни платки, инсталирани на свободните слотове на компютъра сканиращи преди зареждане на операционната система. Въпреки всички тези мерки инвазията на вируси не би могла да бъде предотвратена както поради необходимостта от непрекъснатото обновяване на антивирусния модул, така и от несъвършенствата на операционната система. Не представлява особено голям проблем за хакерите да проникнат в мрежа или компютър. Интернет само им помага, популяризирайки уязвимостта на определена операционна система, давайки възможност без проблем да бъде получен отдалечен или локален достъп до права на администратора. Специализирани сайтове предлагат всевъзможни *lock trash* програми за разбиване и достъп до пароли. Пример в това отношение беше епидемията от вируса *MyDoom*, заразил повече от половината персонални компютри ползващи глобалната мрежа. Смятаната за по-надеждна по отношение на сигурността поне ОС *UNIX* също не успя да избегне проблеми от този род, включително и по-сериозни.

За изключване на възможностите за неоторизирано проникване в компютърните мрежи се използва и комбинирания подход – парола + идентификация на ползвателя чрез персонален „ключ“. Сам по себе си ключът представлява карта (магнитна или с вграден микрочип – смарт карта) или различни устройства за идентификация на ползвателя по биометрични данни – дактилоскопичен отпечатък, ирис на окото, размер на дланта и други. Сървърите и работните станции, снабдени с такива апаратни средства и специализиран софтуер за проверка, значително повишават степента на защита от несанкциониран достъп.

Смарт картите за управление на достъпа позволяват да бъдат контролирани различни функции като логване, достъп до различни устройства на работната станция, до определени програми и фаилове. Един от добрите примери за създаване на комплексни решения за контрол на достъпа е *Kerberos*. Основана на съчетаването на програмни и апаратни средства, тя разчита на три основни компонента за защита:

- База данни, съдържаща информация за всички ресурси на мрежата, ползватели, пароли, информационни ключове и др.
- Сървър за оторизация, чиято основна задача е обработката на заявки на ползвателите на мрежата. Получавайки конкретната заявка за определена мрежова услуга, той се обръща към базата данни и определя пълномощията на ползвателя за извършване на определена операция.
- Сървър за издаване на разрешения. Неговата задача е свързана с получаване на пропуск от Сървъра за оторизация с името на ползвателя и неговия мрежов адрес, време на заявката и уникален ключ. Пакетът, съдържащ пропуска, се предава в зашифрован вид. След разшифроване сървърът сравнява ключовете и дава разрешение за използване на мрежовата апаратура или софтуер.

С разширяване дейността на фирмата, нараства и числеността на абонатите, а появата на нови филиали (по подразбиране не в обсега на конкретната локална мрежа) води до необходимостта за организиране и контрол на отдалечения достъп на ползвателя (група ползватели) до изчислителния ресурс на централния офис.

За организирането на такъв достъп най-често се използват кабелни линии и радиоканали. Във връзка с това защитата на информацията, предавана по канали за отдалечен достъп, изисква специален подход. В мостовете (*bridges*) и маршрутизаторите (*routers*) за отдалечен достъп е необходима сегментация на пакетите – паралелно по две линии. Това прави невъзможно прехващане на данните при незаконно „закачане“ на хакери. Освен това, криптирането и шифрирането на пакетите гарантира още по-висока степен на безопасност на информацията. Мостовете и маршрутизаторите за отдалечен достъп от своя страна са още една бариера пред неправомерния достъп. Те биха могли да бъдат настроени (програмирани) така, че да осигуряват персонален достъп само до определени ресурси на централната база.

Развитието на съвременните технологии за комуникация – GPS (*Global Positioning System*) както и GSM мрежите за предаване на данни предлагат допълнителни възможности за обогатяване на инструментариума, използван за защита на данните и контрол на достъпа в съвременните компютърни мрежи. Идеята за използване на GPS системата се състои в следното: ползвателят на информационния ресурс изпраща своите координати към сателити на системата, намиращи се в зоната на пряка видимост. От своя страна сървърът за автентификация, познаващ орбитите на всички сателити, може да определи местоположението му с голяма точност и да даде разрешение или не за достъп до ресурсите на системата в зависимост от досието му.

Доколкото орбитите на сателитите са подложени на непрекъснати колебания, предсказването на които е достатъчно сложна и трудна задача, фалшифицирането на координатите се оказва практически невъзможно. Няма полза и от прехващане на координатите, тъй като те се променят постоянно. Непрекъснатото предаване на координати не изисква от потребителя някакви допълнителни усилия, поради което той би могъл многократно да потвърждава своята автентичност. GPS апаратурата е сравнително евтина, достатъчно проверена и надеждна. Затова в случаите, в които легалният ползвател трябва да се намира на определено място, този метод за автентификация се оказва доста привлекателен.

Независимо от добрите възможности, предлагани от гореспоменатия метод, той, заедно с този за проверка на биометрични данни, все пак са по възможностите на богати и разполагащи с необходимите средства и възможности фирми и организации. И двата метода се ползват обикновено на места, където се работи със строго секретна и детайлно класифицирана информация.

Развитието на съвременните мобилни комуникации и най-вече на GSM стандарта, позволява ползването на обикновения мобилен телефон като средство за контрол на достъпа до информационния и ресурс във всяка една компютърна мрежа, разполагаща със средства за автентификация. Инвестицията за ползването на такава система не

надхвърля стойността на обикновена работна станция – персонален компютър със стандартни параметри. Необходим е стандартен GSM терминално устройство, свързано със сървъра за автентификация. Устройството е сравнително евтино – почти на цената на нормален GSM апарат. Предлага се от повечето големи фирми производители – *Siemens*, *Nokia* и др., и представлява обикновен апарат без говорител и микрофон (могат да бъдат добавени). Свързва се към сървъра с помощта на RS232 (сериен интерфейс) или обикновен USB при по-новите модификации. За целите на автентификацията на потребителя, в сървъра трябва да бъде добавен елементарен софтуер за приемане и предаване на позвъняване и SMS.

Основната схема на автентификация в корпоративен сървър и мрежа с помощта на мобилни устройства е представена на Фиг. 1.

Фигура 1. Автентификация в корпоративен сървър и мрежа с помощта на мобилни устройства

Принципът на автентификация е базиран на обмен на данни между ползвателя на ресурса посредством личния му мобилен апарат и терминала, инсталиран на сървъра на мрежата. Той може да бъде усложнен и усъвършенстван по усмотрение на администратора, добавяйки към стандартната процедура (приемане/изпращане) на допълнителни данни за проверка като PIN (*Personal Identification Number*) или

допълнителна парола. В основата си обменът включва позвъняване от потребителя, желаещ достъп до системния ресурс. GSM терминалното устройство приема позвъняването и прекъсва връзката (*free call*). Резултатът е получаването на CLIP (*Calling Line Identification Presentation*), съдържащ телефонния номер, включително международния код на потребителя, дата и час на позвъняването. Сървърът проверява за наличието на такъв номер в базата и в зависимост от правата, дефинирани в досието на конкретния потребител, сървърът издава разрешение за достъп до разрешените ресурси на системата. Позвъняването е напълно безплатно за потребителя, тъй като целта е само получаване на CLIP. Верификацията може да бъде усложнена както беше споменато по-горе, ако сигурността го изисква, тъй като апаратът може да бъде откраднат, загубен и т.н. Администраторът би могъл да предвиди някакъв опростен диалог като:

- Опростено логване само на базата на CLIP
- Искане на специален PIN или парола, изпращан от потребителя чрез SMS.
- Генериране на такива от самия сървър (генерирането би могло да включва и времето) и пращането им в SMS на потребителя за последващо логване от работната станция

Използването на този метод за достъп е много надежден с оглед на невъзможността от хакване на пароли и ПИН номера, поради технологията на пренос между сървъра и потребителя – използва се криптирана връзка. От друга страна е лесно приложима и достъпна за почти всяка фирма, независимо от големината ѝ. На трето място не изисква специални устройства от страна на потребителя – в днешни дни насищането с мобилни апарати доближава 100%. Прилагането му в съчетание с други, отработени и проверени такива би допринесло за гарантиране на още по-голяма сигурност в използването на информационния ресурс на фирми и организации и снижаване до минимум опасностите от неправомерен достъп, както и други опасни действия, застрашаващи сигурността на всяко ниво.

ГС приема криптирани транзакции от работните станции или от външни уеб сайтове за е-търговия. Всяка транзакция е определена с време на постъпване и IP на работната станция или уеб сайта.

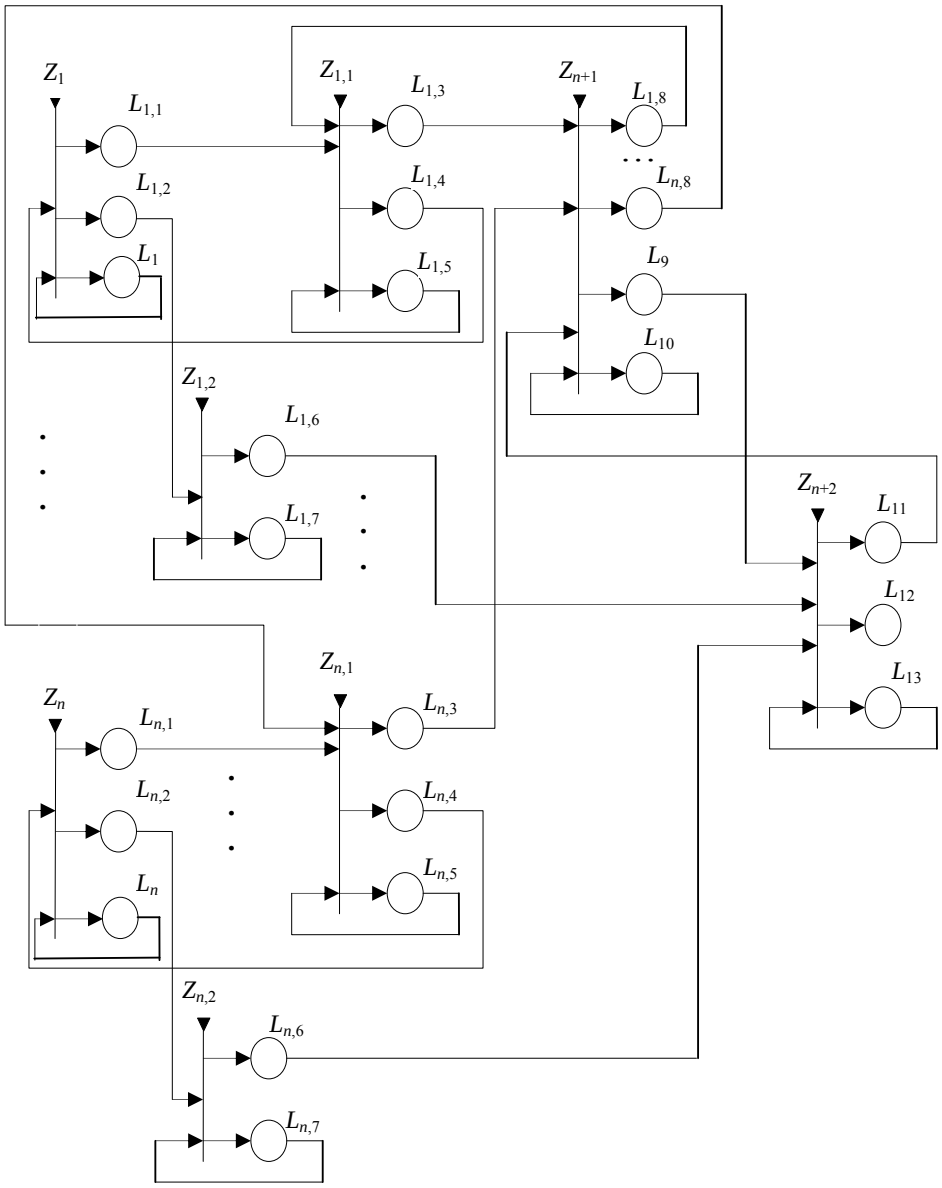
2 Обобщеномрежови модел

Обобщена мрежа [1,2] съдържа следното множество от преходи (Фиг. 2):

$$A= \{ Z_{1,\ldots}, Z_n, Z_{1,1,\ldots}, Z_{n,1}, Z_{1,2,\ldots}, Z_{n,2}, Z_{n+1}, Z_{n+2}\},$$

където преходите представят следните процеси:

- $Z_1,\ldots, Z_n$ – дейностите на клиент i, за $i = 1, 2\ldots, n$,
- $Z_{1,1},\ldots, Z_{n,1}$ – дейностите, свързани с GSM на клиент i, за $i = 1, 2\ldots, n$,
- $Z_{1,2},\ldots, Z_{n,2}$ – дейностите, свързани с компютъра на клиент i, за $i = 1, 2\ldots, n$,
- Z_{n+1} – дейностите, свързани с GSM терминала,
- Z_{n+2} – дейностите, свързани с автентификационния сървър.



Фигура 2. ОМ модел за авторизация на достъпа.

За $i = 1, 2\ldots, n$:

$$Z_i = \{\langle L_i, L_{i,4}\rangle, \langle L_{i,1}, L_{i,2}, L_i\rangle, R_{i,} \vee(L_i, L_{i,4})\},$$

където:

$$R_i = \begin{array}{c|ccc} & L_{i,1} & L_{i,2} & L_i \\ \hline L_i & W_{i,1} & W_{i,2} & True \\ L_{i,4} & False & False & True \end{array},$$

- $W_{i,1}$ = „Клиентът i звъни“,
- $W_{i,2}$ = „Клиентът i праща DEC, криптиран чрез ТМК“.

Ядрото, постъпващо в позиция $L_{i,1}$ не получава нова характеристика. Ядрото, постъпващо в позиция $L_{i,2}$ получава характеристика „DEC“.

За $i = 1, 2\ldots, n$:

$$Z_{i,1} = \{\langle L_{i,1}, L_{i,5}, L_{i,8}\rangle, \langle L_{i,3}, L_{i,4}, L_{i,5}\rangle, R_{i,1,} \vee(L_{i,1}, L_{i,5}, L_{i,8})\},$$

където:

$$R_{i,1} = \begin{array}{c|ccc} & L_{i,3} & L_{i,4} & L_5 \\ \hline L_{i,1} & False & False & True \\ L_{i,5} & W_{i,3} & W_{i,4} & True \\ L_{i,8} & False & False & True \end{array},$$

- $W_{i,3}$ = „От GSM на клиент i се изпраща clip до GSM терминала“,
- $W_{i,4}$ = „От GSM на клиент i се изпраща DEC, криптиран чрез ТМК“.

Ядрата, постъпващи в позиции $L_{i,3}$ и $L_{i,4}$ получават характеристики съответно: „Клиент i, clip“ в позиция $L_{i,3}$, и „Клиент i, DEC“ в позиция $L_{i,4}$.

За $i = 1, 2\ldots, n$:

$$Z_{i,2} = \{\langle L_{i,2,} L_{i,7}\rangle, \langle L_{i,6}, L_{i,7}\rangle, R_{i,2,} \vee(L_{i,2,} L_{i,7})\},$$

$$R_{i,2} = \begin{array}{c|cc} & L_{i,6} & L_{i,7} \\ \hline L_{i,2} & False & True \\ L_{i,7} & W_{i,6} & True \end{array},$$

където $W_{i,6}$ = „Клиент i изпраща данни, криптирани чрез DEC“. Ядрото, постъпващо в позиция $L_{i,6}$ получава характеристика „Клиент i, данни“.

За $i = 1, 2\ldots, n$:

$$Z_{n+1} = \{\langle L_{1,3},\ldots, L_{n,3}, L_{10}, L_{11}\rangle, \langle L_{1,8},\ldots, L_{n,8}, L_9, L_{10}\rangle, R_{n+1,} \vee(L_{1,3},\ldots, L_{n,3,} L_{10}, L_{11})\},$$

където:

$R_{n+1} =$

	$L_{1,8}$	...	$L_{n,8}$	L_9	L_{10}
$L_{1,3}$	*False*	...	*False*	*False*	*True*
...	...	...	...	...	...
$L_{n,3}$	*False*	...	*False*	*False*	*True*
L_{10}	$W_{1,8}$	...	$W_{n,8}$	W_9	*True*
L_{11}	*False*	...	*False*	*False*	*True*

,

- $W_{i,8}$ = „GSM терминалът изпраща DEC на GSM на клиент *i*“, за $i = 1, 2\ldots, n$,
- W_9 = „Изпратен е clip на клиент *i*“.

Ядрата, постъпващи в позиции $L_{1,8},\ldots, L_{n,8}$ получават характеристики съответно: „DEC за GSM на клиент *i*“.

Ядрото, постъпващо в позиция L_9 получава характеристика „Клиент *i*, clip“.

За $i = 1, 2\ldots, n$:

$$Z_{n+2} = \{\langle L_{i,6},\ldots, L_{n,6,}\ L_9, L_{13}\rangle, \langle L_{11}, L_{12}, L_{13}\rangle, R_{n+2,} \vee(L_{i,6},\ldots, L_{n,6,}\ L_9, L_{13})\},$$

където:

$R_{n+2} =$

	L_{11}	L_{12}	L_{13}
$L_{1,6}$	*False*	*False*	*True*
...	...	...	...
$L_{n,6}$	*False*	*False*	*True*
L_9	*False*	*False*	*True*
L_{13}	W_{11}	W_{12}	*True*

,

където W_{11} = „Има неверен clip“. Ядрото, постъпващо в позиция L_{11} получава характеристика „Неверен clip, клиент *i*“.

3 Заключение

Този метод на автентификация премахва единната трансмисия (интернет среда) на предаване на конфиденциални данни – ключове, криптирани данни, пароли за достъп и др., въвеждайки втори канал (GSM комуникация) за предаване на някои от тях. Това значително намалява опасността от неоторизиран или зложелателен достъп.

Инвестициите за допълнително оборудване към сървъра са незначителни – един или няколко GSM терминала. Използването на смартфони от клиентите позволява, част от процеса на авторизация да бъде прехвърлен към мобилното устройство с помощта на подходящи приложения, напр. генериране на ключ за криптиране на данните и предаването му към сървъра през SMS.

Представеният обобщеномрежови модел на автентификация в корпоративен сървър позволява анализ и симулиране на дейностите на клиентите, както и на сървъра с оглед избягване на тесните места във времевата им синхронизация.

С помощта на ОМ модел могат да се формализират ситуации при срив на хардуера в една или двете страни за прецизиране на програмното осигуряване на достъпа.

Представеният обобщеномрежови модел е може да се използва като компонент от по-общи модели, например такива, описващи електронна търговия с мобилни комуникациии и банкови дейности през Интернет [5, 7].

Литература

[1] Atanassov, K., On Generalized Nets Theory, "Prof. M. Drinov"Academic Publishing House, Sofia, 2007.

[2] Atanassov, K., Generalized Nets, World Scientific. Singapore, New Jersey, London, 1991.

[3] Panayotov, H., Generalized net model of the process of avoiding healthcare fraud, Developments in Fuzzy Sets, Intuitionistic Fuzzy Sets, Generalized Nets and Related Topics. Foundations and Applications, Warsaw, Poland, 2011, 185–192.

[4] Panayotov, H., Generalized net model of transaction workflow in GSM based station for e-commerce, Issues in IFS and GNs, Vol. 10, Warsaw, 2013, 152–162.

[5] Kacprzyk, A., I. Mihailov, Intuitionistic fuzzy estimation of the liquidity of the banks: A generalized net model, 13th Int. Workshop on Generalized Nets, London, 29 October 2012, 34–42.

[6] Kodoyannis, V., S. Sotirov, A. Nenov, Modeling of electronic payment by generalized net, Concurrent engineering, The Vision for the future in Research and Application, Portugal, ISBN 90 5809 622 X, 2003, 1043–1046.

[7] Mihailov, I., Generalized Net Model for Describing Some Banking Activities, Proceedings of the, New Developments in Fuzzy Sets, Intuitionistic Fuzzy Sets, Generalized Nets and Related Topics, Vol II: Applications, Warsaw, Poland, 2013, 115–122.

[8] Orozova, D., E. Sotirova, S. Sotirov, Generalized net model of electronic payment processes via Internet, IEEE "Intelligent Systems", 2008, 16-12–16-15.

[9] Sotirova, E., H. Panayotov, M. Krawczak, P. Melo-Pinto, Modeling of e-trade with mobile communications by the apparatus of generalized networks – In Proceedings of the Fifth International Workshop on Generalized Nets, Sofia, 10 Nov. 2004, 41–47.